REMARKS

The Office Action rejected claims 1-2 and 7-20 under 35 U.S.C. 103 as being unpatentable over Claims 1-2, 7-20 are rejected under 35 U.S.C. 1 03(a) as being unpatentable over US Patent Publication Application 2005/0005202 A1 to Burt et al. (the Burt reference) in view of US Patent Publication 2003/0188191 to Aaron et al. (the Aaron reference). However, there are clear errors in the rejection in that neither the Burt reference nor the Aaron reference, either alone or in combination, disclose or suggest the requirements of the claims.

The specification describes a problem in paragraph 6 and 7 of corresponding US Published Application No. 2005/0144314:

> [0006] Given the above-described hierarchy, access to the various router-reported network information is limited to the management system. Thus, if an end user device ("EUD"), or its operator, outside of the management system requires access to such information, such access is provided in an informal manner and is not by way of communications along the actual network. For example, an EUD may represent an operator of an intranet that is connected to the global Internet, where that operator desires information that reflects issues surrounding operation of its intranet insofar as it is networked with the Internet. In this and comparable endeavors, the operator is likely left to making a telephone inquiry to the entity (e.g., carrier, service provider) that oversees the management system (e.g., EMS/NMS), and if responsive the entity must then sort through the raw data of its EMS/NMS databases in an effort to respond to the inquiry. Additionally, by time a response is formulated, hours or even days may pass and, thus, the condition that caused the inquiry may have changed. This process, therefore, includes steps that are not automated, may consume considerable time and human resources, and may produce results that are unreliable and/or stale by time they are received. As such, it may be less than satisfactory for the inquiring entity, particularly if the inquiry is made with respect to a time critical matter.

> [0007] In view of the above, there arises various needs for network management system data to be more readily accessible to entities outside the management system entity, such as EUDs operated by end-users or local operators using the network. These EUDs may well desire to monitor and probe the status and operations of various components of the network and to have insight to traffic statistics such as at router interfaces and accumulated over periodic intervals for a quick snapshot into network activity. For example, the EUD may desire to evaluate the level of compliance of its Internet Service Providers ("ISPs") with a Service Level Agreement ("SLAs") between the ISP and the EUD.

The specification states in part, in paragraph 24 with respect to one embodiment that:

> [0024] . . . For instance, EMS node 28.sub.0 is not part of a management system above line 16, but assume as an example that it desires to have knowledge of certain network traffic statistics in router 18.sub.1, and such certain network traffic statistics are relative to the enterprise network (or intranet) that includes group 26 as well as router 18.sub.2. In this case, the appropriate rule set(s) and desired analysis are provided to EMS node 14.sub.1 and, thus, in the preferred embodiment those aspects are incorporated into a meter manager 60 of EMS node 14.sub.1. In a comparable manner as described above, meter manager 60 informs and controls a meter 52, a meter reader 54, and a non-management system analysis block 56b. Thus, as network traffic passes through router 18.sub.1, its meter 52 monitors that traffic, which is further processed by its meter reader 54 and its non-management system analysis block 56b, consistent with the interests of EMS node 28.sub.0 as indicated in the rule set(s) and analysis it sought. The results are then reported from router 18.sub.1 to EMS node 28.sub.0 through router 18.sub.2 preferably in a form usable by EMS node 28.sub.0, thereby informing EMS node 28.sub.0 of such results in a very short amount of time.

An embodiment describes a router in a service provider network that provides network traffic statistics relative to an enterprise network or intranet that are not part of a management system.

Independent Claim 1 and dependent claims 2 through 19

The Office Action has failed to provide a prima facie case of obviousness for independent claim 1 because it has not shown that the cited references disclose or suggest the elements of claim 1 as explained below.

First, with respect to the Burt reference, the Burt reference fails to disclose or suggest circuitry for in response to receiving a request from a second management system of an end user intranet, processing the provided network information based on a second type of analysis requested by the second management system of the end user intranet. The Burt reference describes a health information system 140 with a customer support system 110. The Burt reference discloses in paragraph 118 that:

> [0118] Referring again to FIG. 2, analyzing module 220 of agent 148 is preferably adapted to receive information gathered by pulling module 210 which are transformed into counters and to compare the counters to the customer-specified thresholds and thresholds specified by customer support system 110 stored in database 240. Analyzing module 220 executes rules 330 to determine what actions need to be taken in response to the comparisons. Actions indicate notifications that need to be sent to customers and customer support system 110 when counters exceed customer thresholds and customer support thresholds.

The customers and customer support system 110 are described in paragraph 24 of the Burt reference:

> [0024] Notifications may be delivered to a designated representative, such as a customer representative, or a customer (user), as desired. The designated representative may be a human or an automated system or process. In one embodiment, the designated representative may be responsible for one or more counters, such that the notification concerning these counters are forwarded to the designated representative. In another embodiment, the designated representative may be responsible for one or more healthcare information systems, such that all notifications concerning these healthcare information systems are forwarded to

> the designated representative. A designated customer representative may be associated with the customer support system 110. That is, for example, the customer support system 110 may have appointed one or more customer representatives who are responsible for one or more counters according to various embodiments.

The Burt reference only describes that customer-specified thresholds and thresholds specified by customer support system 110 are stored in database 240. The customers are described by the Burt reference in paragraph 24 as designated representatives or users of the healthcare information systems 140 that are responsible for the counters in network support of the healthcare information systems 140. There is no description of a service provider wide area network with a first management system or an end user intranet coupled to the wide area network monitored by a second management system. There is no description of receiving a request from a second management system of an end user intranet. There is no description of processing network information based on a second type of analysis requested by the second management system of the end user intranet.

Second, the Burt reference fails to disclose circuitry for transmitting processed network information based on the second type of analysis over a data path in the WAN to at least one node included within the second management system of the end user intranet outside of the first management system, wherein the processed network information based on the second type of analysis provides network information on operation of the WAN affecting operation of the end user intranet. The Burt reference describes in paragraphs 23:

> "[0023] Agent 148 notifies customer support system 110 when the counters or counter instances exceed thresholds specified by customer support system 110 or by users or customers of the healthcare information system. Agent 148 also notifies customers (or customer support system 110) when the counters exceed thresholds specified by customers or users. A user or customer of a healthcare information system refers to, among other things, a doctor, a nurse, a healthcare administrator, or an insurance specialist. Threshold, as used in this disclosure, refers to a value that marks a boundary indicating a level of concern. A threshold

may concern hardware or software system performance as well as business operational status. In various embodiments, thresholds may be predetermined by either the customer support system or the customer (user) of the healthcare information system.

[0024] Notifications may be delivered to a designated representative, such as a customer representative, or a customer (user), as desired. The designated representative may be a human or an automated system or process. In one embodiment, the designated representative may be responsible for one or more counters, such that the notification concerning these counters are forwarded to the designated representative. In another embodiment, the designated representative may be responsible for one or more healthcare information systems, such that all notifications concerning these healthcare information systems are forwarded to the designated representative. A designated customer representative may be associated with the customer support system 110. That is, for example, the customer support system 110 may have appointed one or more customer representatives who are responsible for one or more counters according to various embodiments.

[0025] In one embodiment, the proactive support system 110 further includes an operator capable of performing necessary fixes in response to the notified problems. By repairing the problems, the operator thus brings the value of the counter or counter instance back within the prescribed threshold. The operator may be a human or an automated system or process. The operator may manually or automatically performing the necessary fixes. In certain embodiments, the operator is part of the customer support system. For example, once a notification is acknowledged, the customer support system may repair the customer system, reconfigure the healthcare information system, or send fixes and new updates. In other embodiments, the operator is part of the customer system, which allows the user or customer to respond to the notification of business performance exceptions and adjust business operations accordingly."

As described above, the Burt reference only describes an element/network manager agent 148 in the health care information system that notifies a designated representative in a customer support system responsible for operation of the network or health care information system. There is no description of a second management system of the end user intranet outside of the first management system or transmitting processed network information based on the second type of analysis that provides network information on operation of the WAN affecting operation of the end user intranet.

The Aaron reference also fails to disclose or suggest these elements of claim 1. The Aaron reference states in paragraph 40:

> [0040] FIG. 2 shows in, schematic form, a computer network-system including an intrusion detection system in accordance with the present invention. A plurality of network devices such as hosts, servers, and personal computers attached within customer site networks (shown here as customer site networks 220, 230, 240, 250), are shown coupled to an intervening computer network 204, such as a public network like the Internet. Routers (not shown) are typically used in the coupling. The customer site networks represent "internal" protected networks local to a particular corporation or site, for example. The customer site networks may or may not be publicly accessible or may comprise a publicly accessible network and an internal "private" network. Each customer site network or LAN (Local Area Network) comprises one or more hosts (e.g., customer site network 220 is shown with hosts 224, 226; customer site network 230 is shown with host 234; customer site network 240 is shown with hosts 244, 246; and customer site network 250 is shown with hosts 254, 256). Each site network is connected to the intervening computer network 204 via a firewall (e.g., host 220 is shown with firewall 221; host 230 is shown with firewall 231; host 240 is shown with firewall 241; and host 250 is shown with firewall 251).

The Aaron reference describes performing intrusion detection in paragraph 44-48:

> [0044] The system performs broad-scope intrusion detection by monitoring the communications on a network or on a particular segment of the network. The data collection and processing center [205] receives information from the various network devices attached to the computer network 204. For example, all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center. Thus, the data collection and processing center receives all communications (i.e., the data) originating from a user on the computer network 204 and flowing to host 220 (and vice versa), for example, as well as all communications originating from the computer network 204 and flowing to all other hosts (and vice versa).
>
> . . . .
>
> [0048] The present invention provides aggregate traffic/intrusion monitoring in the provider network. This allows for a broader scope of network activity to be considered and analyzed, not just relevant to a single customer, but across some or all customers. The additional data is valuable because the probing/reconnaissance activities of would-be intruders typically cover a large number of customers, so as to select those with security weaknesses for more in-depth attack. Additional patterns of broadly suspicious activity can thus be correlated/recognized across many customers.

The Aaron reference fails to describe that the hosts 220, 230, 240, 250 are able to transmit a request to the computer network 204 for processed network information based on a second type of analysis that provides network information on operation of the WAN affecting operation of the end user intranet.

Combination Teaches Same Problem

Furthermore, the combination of the Aaron reference and the Burt reference fails to suggest the elements, *inter alia*, of claim 1 of, "circuitry for processing the provided network

information based on a first type of analysis requested by the first management system and in response to receiving a request from the second management system of the end user intranet, processing the provided network information based on a second type of analysis requested by the second management system of the end user intranet; and circuitry for including processed network information based on the second type of analysis into one or more packets; and circuitry for transmitting processed network information based on the first type of analysis to the first management system and transmitting the one or more packets with processed network information based on the second type of analysis over a data path in the WAN to at least one node included within the second management system of the end user intranet outside of the first management system, wherein the processed network information based on the second type of analysis provides network information on operation of the WAN affecting operation of the end user intranet. The combination of the Aaron reference and the Burt reference teaches away from the elements of claim 1. The Burt reference teaches that only designated representatives of a health information system responsible for the network support of the health information system are provided alerts of predetermined thresholds. Similarly the Aaron reference only discloses that a central data processing center 205 of a computer network 204 provides aggregate traffic/intrusion monitoring of data communications in the computer network 204.

Accordingly, the combined teachings of Aaron reference and the Burt reference fail to teach or suggest the requirements of claim 1. As a dependent claims to claim 1, claims 2 through 5 and 7 through 19 add further patentable matter to claim 1 and thus are further differentiated and patentable under 35 U.S.C. §103 over the Aaron reference in view of the Burt reference.

Independent Claim 21 and dependent Claim 22

For similar reasons stated with respect to claim 1, the combined teachings of Aaron reference and the Burt reference fail to teach or suggest the requirements of claim 21. As a dependent claim to claim 21, claim 22 adds further patentable matter to claim 21 and thus is further differentiated and patentable under 35 U.S.C. §103 over the Aaron reference in view of the Burt reference.

CONCLUSION

For the above reasons, the foregoing amendment places the Application in condition for allowance. Therefore, it is respectfully requested that the rejection of the claims be withdrawn and full allowance granted. Should the Examiner have any further comments or suggestions, please contact Jessica Smith at (972) 240-5324.

Respectfully submitted,

GARLICK HARRISON & MARKISON

Dated: April 6, 2009

/Jessica Smith/

Jessica W. Smith
Reg. No. 39,884

Garlick Harrison & Markison
P. O. Box 160727
Austin, TX 78716-0727
Phone: (972) 240-5324
Fax: (888) 456-7824